REMARKS

Applicant thanks the Examiner for carefully considering this application, and for the courtesies extended during the Examiner Interview of February 3, 2011. Additionally, Applicant thanks the Examiner for indicating during the Examiner interview that, upon receipt of the present amendments to the claims, the rejections under 35 U.S.C. §102 would be withdrawn. Please reconsider the application in view of the above amendments and the following remarks.

Disposition of Claims

Claims 1-13 and 15-20 are currently pending. Claims 1 and 15 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 15.

Claim Amendments

Independent claims 1 and 15 are amended by way of this reply, to more precisely claim the present invention. Support for the amendments can be found, for example, in paragraphs [0050]-[0052] of the publication of the present application (U.S. Patent Application Publication No. 2007/0253551). No new matter is added by way of these amendments.

Rejection(s) under 35 U.S.C. § 102

Claims 1-7, 11-13, 15-16, and 19-20 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,286,103 ("Maillard"). Claims 1 and 15 have been amended by way of this reply. To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

Referring to Fig. 3 of the present application as an example, the system and method of the claimed invention comprises a broadcasting network having a plurality of receiving decoding systems 301_i. Each receiving decoding system 301_i includes a decoder 303_i

having a unique first key K_{i1} assigned thereto, and a portable security module 302_i having a second key K_{i2}, which is determined according to the first key K_{i1}, assigned thereto. A broadcasting center sends out a common pairing system key K_{PS} to each receiving decoding system, and the combination of the first and the second keys K_{i1}, K_{i2} for each receiving unit is congruent to the pairing system key K_{PS}. The congruence, when validated, allows for decryption of encrypted control data.

The first key K_{i1} and second key K_{i2} are unique for each receiving unit, and the second key K_{i2} is determined according to the first key K_{i1} and, therefore, a subscriber cannot lend the portable security module 302_i to another receiving unit, because the second key K_{i2} of each receiving decoding systems 301_i must be combined with the *corresponding* first key K_{i1} for the combination to be congruent to the pairing system key K_{PS}. Additionally, because a common pairing system key K_{PS} is sent to the plurality of receiving decoding systems 301_i, a new pairing system key K_{PS} can be sent much more often than in other systems where a different pairing key is required to be sent for each receiving decoding system. Thus, the validation can occur more often, which prevents people from hacking a decoder key to pirate the pairing key of the decoding system, because the paring key would only be valid for a short period of time. *See*, e.g., paragraphs [0050]-[0062] of the specification of the published application.

Accordingly, amended independent claim 1 requires, in part, "selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network," and "determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data." Amended independent claim 15 requires, in part, "a decoder to which is assigned a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network; a portable security module to which is assigned a second key, wherein the decoder and the portable security module form a pairing system," "wherein the second key is determined according to the first key such that a combination of the first key and the second key is congruent to a pairing system key which enables decryption of broadcasted encrypted control data that is received by each receiving decoding system."

Maillard discloses a conditional access system having a scrambled audiovisual data stream received by a decoder 3020, and passed to a portable security module 2020. At the portable security module 202, the data stream is descrambled by a descrambler 3030 using the exploitation key Cex possessed by the portable security module 3020 to generate the decrypted control word CW. Then, the transmission is descrabled. The descrambled data stream is re-encrypted according to a first encryption key Kf at 3031, then passed to the decoder 2020, which decrypts the descrambled data scream using the key Kf and identity value N. In Maillard, the exploitation key Cex is encrypted based on a personalization key corresponding to a decoder identity value N that is uniquely associated with the identity of each decoder. Thus, the transmitter sends the exploitation key Cex to the portable security module 3020 via an EMM that is unique to each portable security module 3020. That is, the transmitter has a database of all personalisation keys held by each portable security module 3020, and sends the unique EMM to each portable security module 3020 that corresponds to the unique corresponding personalisation key of the decoder. (*See* Fig. 3 and line 13 of column 8 to line 17 of column 9 of Millard.)

The system of Maillard differs from the claimed invention in at least two ways. First, because the EMM containing the exploitation key Cex depends on the personalisation key that corresponds to the unique decoder identity value N, a different EMM is sent to each portable security module 3020. Thus, there is no single pairing system key that is *common* to each receiving decoding system in Maillard. In fact, as described above, the system of Maillard is not set up to send a common key to multiple receiving units with a decoder and portable security module paired together. This is significant because sending a *different EMM* to each portable security module 3020 requires a large array of EMM's, which in turn requires a large amount of time to send each array of EMM's. Thus, the frequency of validation using the EMM is greatly reduced. In fact, Maillard states that the exploitation key Cex is only changed once a month. (*See* line 65 of column 7 to line 2 of column 8 of Maillard.)

Additionally, the Examiner cites "Maillard, Col. 8 Lines 55 - 63, key pair for decoder and smart card," which discusses a private/public key pairing, as disclosing the pairing system key being common to each receiving decoding system. However, Applicant notes that, although the embodiment shown in Fig. 4 discloses a public key Kpub, Maillard fails to teach the public key Kpub being *common* to multiple receiving decoding systems. (*See* Fig. 4 and line 18 of column 9 to line 17 of column 9 of Millard.)

Second, Maillard does not validate a combination of the encryption key Kf of the portable security module 3020 and the decryption key Kf of the decoder 2020 by checking for congruence of the combination thereof to a pairing system key. In fact, it appears that Maillard does not send any keys to the portable security module 3020 for the purpose of validating the pairing of the encryption key Kf of the portable security module 3020 and the decryption key Kf of the decoder 2020. Thus, Maillard does not prevent decryption if there is lack of congruence with a pairing system key. Instead, the encryption/decryption process proceeds as long as the decryption key Kf of the decoder 2020 can decrypt the encryption of the encryption key Kf of the portable security module 3020. Said another way, the claimed invention requires three interconnected keys: a first key unique to a single device, a second key that is determined based on the first key, and a pairing system key to which a combination of the first key and the second key must be congruent in order for the first/second key combination to be validated. In contrast, Maillard has an encryption key Kf and a decryption key Kf, whose pairing is never validated. Instead, upon initialization of the decoder, Maillard simply sends the unique encryption key Kf to the portable security module 3020 based on the decoder identity value N of the decoder 2020, and the validation of the pairing is never verified thereafter. Thus, a hacked encryption/decryption key Kf would be valid indefinitely in Maillard. Accordingly, Maillard fails to anticipated the aforementioned limitations of amended claims 1 and 15.

Additionally, the Examiner cites "Maillard, Col. 8 Lines 55 - 63, key pair for decoder and smart card," which discusses a private/public key pairing, as disclosing the combination of the first key and the second key being congruent to a pairing system key. However, Applicant notes that, although the embodiment shown in Fig. 4 discloses a public key Kpub, the system of Maillard does not check for congruence of the public key Kpub with the encryption key Kf and the decryption key Kf. Instead, the public key Kpub is employed to encrypt the pseudo-random number RN generated by the decoder 202, to be decrypted by the private key Kpri stored on the portable security module 3020. In fact, the only connection that the encryption key Kf and the decryption key Kf have with the public key Kpub is that the pseudo-random number RN encrypted by the public key Kpub and decrypted by the private key Kpri is received by the encryption key Kf in the portable security module 3020. Thus, the system of Maillard clearly does not check for congruence of the public key with the encryption key Kf and the decryption key Kf. (*See* Fig. 4 and line 18 of column 9 to line 17 of column 9 of Millard.)

In view of the above, claims 1 and 15 are patentable over Maillard, at least for the above reasons. Claims 2-7, 11-13, 16, and 19-20 depend, either directly or indirectly, from claims 1 and 15, and are patentable over Maillard, at least for the same reasons as claims 1 and 15. Accordingly, withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C. § 103

Claims 7-10, 17, and 18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Maillard in view of U.S. Patent Application Publication. No. 2001/0002486 ("Kocher"). Claims 1 and 15 have been amended by way of this reply. To the extent that this rejection may still apply, this rejection is respectfully traversed.

As explained above, Maillard fails to show or suggest all of the limitations of independent claims 1 and 15. Kocher fails to supply that which Maillard lacks. Specifically, Kocher discloses an RSA encryption/decryption algorithm. However, Kocher fails to show or suggest a single pairing system key that is *common* to each receiving decoding system, or a first key, a second key determined according to the first key, and a pairing system key to which the combination of the first and second keys must be congruent for decryption to occur.

In view of the above, independent claims 1 and 15 are patentable over Maillard and Kocher, whether considered alone or in combination, at least for the above reasons. Claims 7-10 and 17-18 are dependent, either directly or indirectly, from claims 1 and 15, and are patentable over Maillard and Kocher, at least for the same reasons as claims 1 and 15. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 17250/017001).

Dated: February 14, 2011

Respectfully submitted,

By Seema Mehta
for Jonathan P. Osha 56,235
Registration No.: 33,986
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant